⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1-122227

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)5月15日
H 04 K 1/00		Z-7240-5K	
H 04 L 9/00		Z-7240-5K	
H 04 N 1/44		6940-5C	審査請求　未請求　発明の数 1　(全6頁)

㊹発明の名称　伝送装置

㉑特　願　昭62-280382
㉒出　願　昭62(1987)11月6日

㉜発明者　竹内　得晴　東京都新宿区西新宿1丁目26番2号　ユニカ株式会社内
㉜発明者　石井　秀治　東京都新宿区西新宿1丁目26番2号　コニカ株式会社内
㉛出願人　コニカ株式会社　東京都新宿区西新宿1丁目26番2号
㉞代理人　弁理士　山口　邦夫

明　細　書

1．発明の名称

伝　送　装　置

2．特許請求の範囲

(1)伝送すべき情報信号の機密性を図るために設けられた、暗号強度の異なる複数の暗号化手段と、

これら複数の暗号化手段を選択する選択手段とを有し、

上記情報信号の機密性に応じて上記暗号化手段が選択されるようになされたことを特徴とする伝送装置。

3．発明の詳細な説明

[産業上の利用分野]

この発明は、ファクシミリ装置等のように回線を利用して情報信号の授受を行なうようにした伝送装置、特に機密機能を有する伝送装置に関する。

[発明の背景]

ファクシミリ装置等のように回線を利用して情報信号の伝達を行なうようにした伝送装置においては、伝送すべき情報信号が機密性に富むものである場合には、これを目的とする個所にのみ機密性を保持したまま伝送する必要がある。

このような要求に答えるものとして、従来から情報信号を暗号化して伝送するようにした装置が開発されている。

このような暗号化機能を有するファクシミリ装置の一例を第8図を参照して説明する。

端子1には、情報信号(文書等)が供給され、これがA/D変換器2において所定のディジタル信号に変換された後、暗号化装置3により所定の暗号化処理が施される。

暗号化された情報信号は、変調器7において伝送形態に適した信号に変換された後、端子8を通して回線(図示せず)に送出される。

暗号化装置3は図示するように、単一の暗号化手段3Aと、その前段及び後段に設けられた一対の選択スイッチ4，5を有する。

そして、端子６に加えられる制御信号によって情報信号の暗号化の有無が選択され、暗号化しようとする場合には一対の選択スイッチ４，５は図示のように切り換えられる。これによって情報信号に所定の暗号化処理が施される。

受信側では、この暗号化された情報信号を所定の手順に基づいて復合することにより、所定の情報信号が再現されることになる。

［発明が解決しようとする問題点］

ところで、このように送信側において、暗号化装置３を設け情報信号に対し、所定の暗号化処理を施して伝送するように構成する場合、従来においては単一の暗号化手段３Ａが設けられているに過ぎないから、その情報信号の機密性の程度に応じた適切な暗号化処理を行なえない欠点があった。

すなわち、文書の機密性に応じて暗号強度を制御すれば、それだけ高精度の暗号化処理が行なわれたことになるからである。

通常、極秘、社内秘、部内秘等のように機密性にランク付けされるのが普通であるから、このような機密性の程度に応じてその暗号強度を変更できるようにすれば、伝送される情報信号の機密性がより高められることは明らかである。

しかし、従来においては単一の暗号化手段３Ａのみを有するため、文書の機密性に対応した暗号化を行なうことができないと言う欠点があった。

そこで、この発明においては文書の機密性の程度に対応できるようにした暗号化機能を有する伝送装置を提案するものである。

［問題点を解決するための技術的手段］

上述の問題点を解決するため、この発明においては、伝送すべき情報信号の機密性を図るために設けられた、暗号強度の異なる複数の暗号化手段と、

これら複数の暗号化手段を選択する選択手段とを有し、

情報信号の機密性に応じて暗号化手段が選択されるようになされたことを特徴とするものである。

［作　用］

ユーザによって、暗号強度の内容が選択される。これに基づき、暗号強度の異なる複数の暗号化手段が選択される。

従って、文書の機密性に応じた暗号化手段を選択すれば、それに応じた機密性を確保できるから、情報の漏洩等の問題を一掃することができる。

例えば、社内秘等のような比較的機密性が低い文書を伝送するような場合には、暗号強度の弱い暗号化手段を選択すればよく、また、最高に機密性を保つ必要がある場合には、最も強い暗号強度の暗号化手段を選択すればよい。

こうすることによって、要求される機密性に対処した伝送が実施され、情報の漏洩の問題を一挙に解決できる。

［実　施　例］

続いて、この発明に係る伝送装置の一例を上述したファクシミリ装置に適用した場合につき、第１図以下を参照して詳細に説明する。

第１図において、端子１に供給された情報信号（文書等の信号）は、Ａ／Ｄ変換器２において所定のディジタル信号に変換された後、暗号化装置３において所定の暗号化処理が施される。

暗号化処理が施された情報信号は、変調器７において所定形態の信号に変換された後、端子８を通じて回線側に送出される。

暗号化装置３は図示するように暗号強度の異なる複数、この例では３個の暗号化手段３Ａ～３Ｃが設けられ、夫々が一対の選択スイッチ４，５によって選択されるようになされている。どの暗号化手段を選択するかは、端子６に供給された選択信号に基づいて選択される。

第２図は暗号化手段３Ａの一例を示すものであって、端子２１には暗号化キーＫ１が供給される。この暗号化キーＫ１はオペレータ側が自由に選択するキーコードである。

この暗号化キーＫ１は暗号回路２２において、換字すなわち暗号化される。暗号化後の暗号化キーＫｅはさらに暗号回路２３に供給されることにより、端子２４に供給された画像信号が、この暗号化キーＫｅに基づいて、この暗号化キーＫｅに対応した所定の暗号化処理が行なわれることになる。

暗号回路２３で暗号化された情報信号は、さらにその機密性を確保するために、後段の暗号回路２５に供給され、ここに加えられた第２の暗号化キーK2によってさらに暗号化処理が施される。実施例ではさらに加算器２６が設けられ、ここにおいて第３の暗号化キーK3が付加される。第３の暗号化キーK3の付加によって暗号化処理が終了する。

ここで、第２及び第３の暗号化キーK2，K3は固定である。

従って、情報信号のみならず暗号化キーK1そのものも暗号化され、また数段にわたる暗号化処理が施されるため、これによって一層の機密性が保持されることになる。

情報信号をどのように暗号化するかによって、その暗号強度が相違する。

例えば、データの置換のみの暗号化に対して、データの置換と、その並べ換えを行なうような暗号化処理の場合には、前者より後者の方が暗号強度が強い。

どのような暗号強度とするかは、暗号回路２２によって変わるので、暗号化手段３A～３Cによってその暗号回路２２及び２３の内容が相違する。

このように所定の暗号強度を持つ暗号化された情報信号は、受信されることによって復号されるが、その復号化手段３０Aの一例を第３図に示す。

端子３１に入力した情報信号すなわち暗号文は、加算器３２において第３の暗号化キーK3が付加され、その状態で復号回路３３に供給されることにより、これに加えられた第２の暗号化キーK2に基づいて最初の復号化処理が行なわれる。

そして、最終段の復号回路３４には暗号化キーKeが供給され、この暗号化キーKeによって、情報信号が最終的に復号される。

なお、この復号化手段３０A側にも、第１の暗号化キーK1をKeに暗号化した復号回路３５が設けられている。

第４図は単一の暗号化手段３Aのみによってもその暗号強度を異ならしめることにより、複数の暗号化手段を使用したと同様の機能を達成できるようにしたものである。

そのため、暗号化装置３においては第１図に示した暗号化手段のうち適当な手段、例えば暗号化手段３Aが使用され、これが選択スイッチ４，５によって選択される。

そして、暗号化手段３Aにはその暗号強度を変更する変更手段１１が設けられている。この例では第１の暗号化キーK1の桁数を変更することによって、暗号強度を異ならしめたと同様の機能を付与している。

すなわち、第５図に示すように暗号化キーK1は、複数の暗号強度、この例では３段階に分けられた暗号強度を持つように設定されている。

すなわち、レベル１の場合には、暗号化キーK1はK11となされ、レベル２の場合には暗号化キーK11とK12を合わせたものが使用される。

レベル３に至ってはこれら暗号化キーK11，K12の他にK13という暗号化キーが使用され、これら桁数の相違に基づいて異なった暗号処理が行なわれることになる。

どのような桁数の暗号化キーを選択するかは、端子１２に供給される選択信号によって変わる。

通常は、暗号化キーの桁数が多くなればなるほど暗号強度が強くなるため、それらはより高度な機密性を要求される場合に使用されることになる。

例えば、レベル１の場合は社内秘であり、レベル２の場合は部内秘であり、レベル３の場合は極秘というように、段階的に便宜的に分ければ、これらによって、夫々機密性の程度が相違し、必要にしてかつ充分な機密性を得ることができる。

このように、暗号化キーK1の内容を選択できるようにした場合には、グループ別にその機密性を持たせることが可能になる。すなわち、伝送すべき情報信号のグループ化を達成することができる。

例えば、第６図に示すようにグループを３段階に分け、グループAを最も機密性の高い極秘とし、グループBは部内秘、グループCは社内秘というようにグループ分けをしたものとすれば、極秘文書を伝送するにはレベル３の暗号化キーK1を選

択すればよい。こうすることによって、極秘文書はグループＡ内のみその授受が可能となる。

これに対して暗号化キーＫ1としてレベル２のものを選択した場合には、グループＡ同士の信号伝達は可能になると共に、グループＢ同士の間における信号の伝達も可能になる。さらにグループＡＢ間における情報の伝達も可能になる。しかし、グループＣとの情報の伝達はできない。

しかしながら、レベル１の暗号化キーＫ1を選択した場合には、これら３つのグループの相互間において情報の伝達が可能になるから、機密性に応じてグループ別による通信が可能になるため、より一層の機密性を保持することができる。

このようなグループ化を実現するには、夫々のグループに対応して暗号化キーの形成及び解読できる手段が設けられることになる。

これによって、第６図に示すようにそのグループごとに受信端末側において、どのレベルの暗号化キーを受信できるかが自動的に認識され、送信側で指定されたレベル以下の機能しか持たない受信端末に対しては、伝送された情報信号が復号化できなくなって通信内容の漏洩が防止される。

第７図は、この発明のさらに他の例を示すものであって、この第７図の実施例は第１図の実施例と第４図の実施例を組合せたものである。すなわち、暗号化装置３としては暗号強度の異なる複数の暗号化手段３Ａ～３Ｃが設けられると共に、その夫々について暗号化キーのレベルが選択できるように構成されている。

このような構成にした場合には、伝送すべき情報信号の機密性をより一層確実に確保することができる。

［発明の効果］

以上説明したように、この発明の構成においては、送信側において文書の機密性を指定することによりその文書に適した暗号強度を持つ暗号化を達成できるようにしたものである。

すなわち、送信側においては、伝送すべき情報信号の機密化を図るために暗号強度の異なる複数の暗号化手段が設けられたものであって、情報信号の機密性に応じて複数の暗号化手段が自由に選択できるようにしたものである。

この構成によれば、文書の機密性に応じた暗号化処理が達成できるので、伝送された情報信号の漏洩をほぼ確実に回避できる特徴を有する。

従って、この発明に係る伝送装置は上述したように、伝送すべき情報信号に対する機密性が要求されるファクシミリ装置等に適用して極めて好適である。

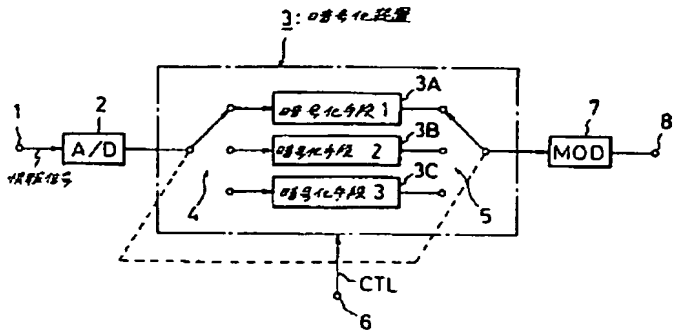
４．図面の簡単な説明

第１図はこの発明に係る伝送装置の一例を示す要部の系統図、第２図は暗号化手段の一例を示す系統図、第３図は復号化手段の一例を示す系統図、第４図はこの発明の他の例を示す伝送装置の系統図、第５図は暗号化キーの説明図、第６図はグループ別通信の説明図、第７図はこの発明に係る伝送装置のさらに他の例を示す系統図、第８図は従来の伝送装置の一例を示す系統図である。

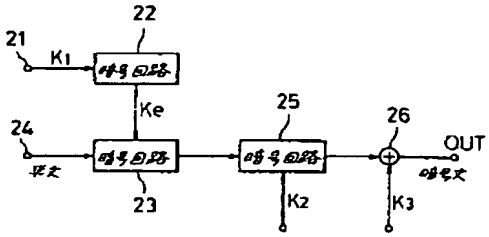
２・・・Ａ／Ｄ変換器
３・・・暗号化装置
３Ａ～３Ｃ・・・暗号化手段
７・・・変調器
１１・・・選択手段
２２，２３，２５・・・暗号回路
３３，３４，３５・・・復号回路

特許出願人　コニカ株式会社
代理人　弁理士　山口邦夫

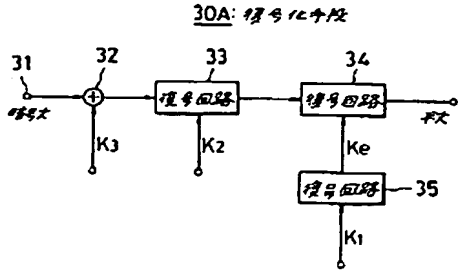
第1図



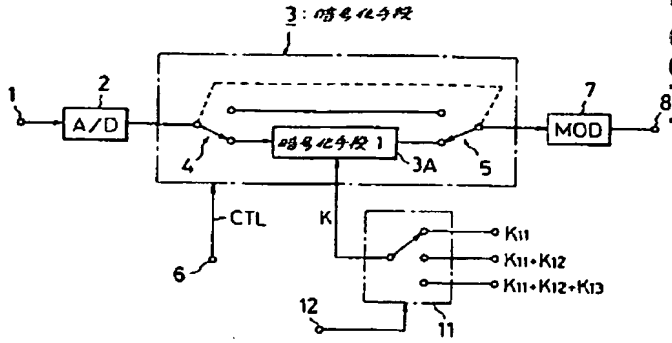
第2図



第3図

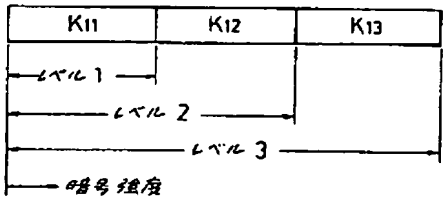


第4図

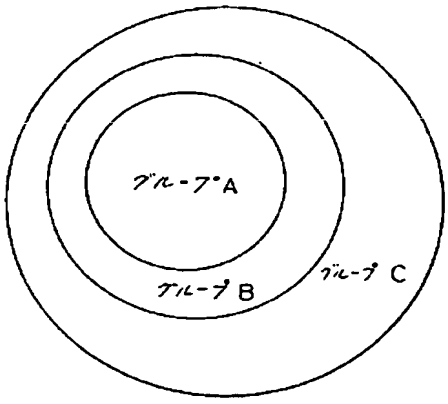


第5図

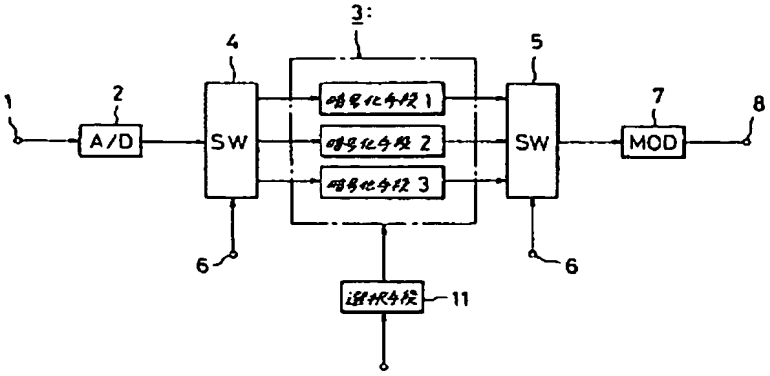
K1：暗号化キー



第6図



第7図



第8図